

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Attorney Docket No. 249/387

In re patent application of

Kyung-hun JANG, et al.

Group Art Unit: (Unassigned)

Serial No. (Unassigned)

Examiner: (Unassigned)

Filed: Concurrently

For: CRYPTOGRAPHIC METHOD USING DUAL ENCRYPTION KEYS AND A
WIRELESS LOCAL AREA NETWORK (LAN) SYSTEM THEREFOR

CLAIM FOR CONVENTION PRIORITY

Commissioner for Patents
P.O. Box 1450
Alexandria, VA. 22313-1450

Sir:

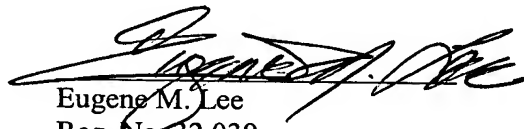
The benefit of the filing date of the following prior foreign application filed in the following foreign country is hereby requested, and the right of priority provided in 35 U.S.C. § 119 is hereby claimed.

In support of this claim, filed herewith is a certified copy of said original foreign application:

Korean Application No. 2002-39156, filed July 6, 2002.

Respectfully submitted,

July 7, 2003
Date


Eugene M. Lee
Reg. No. 32,039
Richard A. Sterba
Reg. No. 43,162

LEE & STERBA, P.C.
1101 Wilson Boulevard Suite 2000
Arlington, VA 20009
Telephone: (703) 525-0978

대한민국 특허청

KOREAN INTELLECTUAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto
is a true copy from the records of the Korean Intellectual
Property Office.

출원번호 : 10-2002-0039156
Application Number

출원년월일 : 2002년 07월 06일
Date of Application JUL 06, 2002

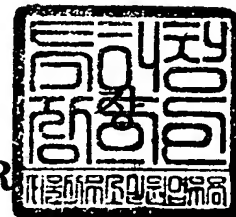
출원인 : 삼성전자주식회사
Applicant(s) SAMSUNG ELECTRONICS CO., LTD.



2003 03 20
 년 월 일

특 허 청

COMMISSIONER



【서지사항】

【서류명】	특허출원서
【권리구분】	특허
【수신처】	특허청장
【참조번호】	0009
【제출일자】	2002.07.06
【국제특허분류】	H04L
【발명의 명칭】	이중키를 이용한 암호화방법 및 이를 위한 무선 랜 시스템
【발명의 영문명칭】	Cryptographic method using dual encryption keys and wireless local area network system therefor
【출원인】	
【명칭】	삼성전자 주식회사
【출원인코드】	1-1998-104271-3
【대리인】	
【성명】	이영필
【대리인코드】	9-1998-000334-6
【포괄위임등록번호】	1999-009556-9
【대리인】	
【성명】	이해영
【대리인코드】	9-1999-000227-4
【포괄위임등록번호】	2000-002816-9
【발명자】	
【성명의 국문표기】	장경훈
【성명의 영문표기】	JANG, Kyung Hun
【주민등록번호】	700228-1405318
【우편번호】	442-470
【주소】	경기도 수원시 팔달구 영통동 968 신나무실 동보아파트 621동 601호
【국적】	KR
【발명자】	
【성명의 국문표기】	박종애
【성명의 영문표기】	PARK, Jong Ae
【주민등록번호】	650814-2453511

【우편번호】 137-930
【주소】 서울특별시 서초구 반포1동 반포주공아파트 346동 203호
【국적】 KR
【발명자】
【성명의 국문표기】 이인선
【성명의 영문표기】 LEE, In Sun
【주민등록번호】 711028-2030218
【우편번호】 140-731
【주소】 서울특별시 용산구 이태원2동 청화아파트 9동 1102호
【국적】 KR
【취지】 특허법 제42조의 규정에 의하여 위와 같이 출원합니다. 다
 리인 이영
 필 (인) 대리인
 이해영 (인)
【수수료】
【기본출원료】 20 면 29,000 원
【가산출원료】 0 면 0 원
【우선권주장료】 0 건 0 원
【심사청구료】 0 항 0 원
【합계】 29,000 원
【첨부서류】 1. 요약서·명세서(도면)_1통

【요약서】

【요약】

이중키를 이용한 암호화방법 및 이를 위한 무선 랜 시스템이 개시된다. 이러한 이중키를 이용한 암호화방법은 하나의 애드-혹 그룹을 구성하는 N개의 무선단말(여기서 N은 2 이상의 양수)중 키분배센터 역할을 담당하는 메인 무선단말을 설정하는 단계; 상기 N개의 무선단말에서 그룹 패스워드를 이용하여 제1 공유키를 생성하는 제1 공유키 생성단계; 상기 메인 무선단말에서 무선단말들간의 데이터 전송시 사용되는 제2 공유키를 생성하는 제2 공유키 생성단계; 상기 메인 무선단말에서 상기 제2 공유키를 상기 제1 공유키로 암호화하여 (N-1)개의 무선단말로 전송하는 제2 공유키 전송단계; 및 상기 N개의 무선단말간에 상기 제2 공유키로 데이터를 암호화하여 전송하는 데이터 전송단계로 이루어진다. 이에 따르면, 애드-혹망 무선 랜 시스템에 있어서 사용빈도가 적은 제1 공유키를 그룹 패스워드를 이용하여 생성하고, 데이터전송시 사용되는 제2 공유키를 랜덤 키 생성 알고리즘에 따라서 키분배센터 역할을 하는 무선단말에서 생성/분배/변경함으로써 데이터의 비밀성을 보장할 수 있다.

【대표도】

도 2

【명세서】**【발명의 명칭】**

이중키를 이용한 암호화방법 및 이를 위한 무선 랜 시스템{Cryptographic method using dual encryption keys and wireless local area network system therefor}

【도면의 간단한 설명】

도 1은 일반적인 애드혹망 무선 랜 시스템에 있어서 암호화방식을 설명하기 위한 도면,

도 2는 애드혹망 무선 랜 시스템에 있어서 본 발명에 따른 이중키를 이용한 암호화 방법을 설명하는 흐름도,

도 3은 본 발명에 따른 제2 공유키 변경방법을 설명하는 흐름도,

도 4는 애드혹망 무선 랜 시스템에 있어서 본 발명에 따른 무선단말의 구조를 보여주는 세부블럭도,

도 5는 도 4에 있어서 각 부의 작동관계를 설명하는 도면이다.

*도면의 주요부분에 대한 부호의 설명

41,45 ... 무선단말 42,46 ... 제1 공유키 생성부

43,47 ... 암호화부 44,48 ... 키관리부

【발명의 상세한 설명】**【발명의 목적】****【발명이 속하는 기술분야 및 그 분야의 종래기술】**

- <9> 본 발명은 무선 랜 시스템에 관한 것으로, 특히 애드-혹망 무선 랜 시스템에 있어서 제1 공유키 및 제2 공유키로 이루어진 이중키를 이용하여 암호화함으로써 보안을 강화시킨 이중키를 이용한 암호화방법 및 이를 위한 무선 랜 시스템에 관한 것이다.
- <10> 일반적으로 무선 랜 시스템은 유선 랜과 독립적으로 무선 NIC를 장착한 복수의 단말들끼리 단독으로 연결하는 애드-혹(Ad-Hoc) 망과, 무선 접속노드를 통해 무선 단말을 유선 랜에 연결하는 인프라스트럭처(Infrastructure) 망 방식으로 구성되어진다. 애드-혹망은 네트워크 기능을 가지고 있는 2개 이상의 무선단말이 모여서 이루어지며, 인프라스트럭처망과는 달리 다른 무선단말로의 연결을 제공하기 위한 고정된 무선 접속노드를 갖지 않는다. 애드-혹망의 각 무선단말은 SSID(service set identifier)를 같게 하면 연결될 수 있는 거리 안에 있는 것은 하나의 애드-혹 그룹이 되어 서로 인식할 수 있으며, 하나의 무선단말이 인터넷에 연결되어 있으면 그 무선단말이 서버가 되어 같은 애드-혹 그룹에 묶여 있는 다른 무선단말에서도 인터넷 공유 프로그램이나 윈도우즈의 공유 메뉴로 인터넷을 나눠 쓸 수 있다. 이러한 애드-혹망은 통상 공통 관심사를 갖는 특정 사용자들에 의해 형성되며, 그룹내 정보는 대체적으로 사적인 경향이 있고, 특정 목적에 따라 일시적으로 발생하므로 지속성이 없다는 특징이 있다. 또한, 애드-혹 망에서는 생성자가 일시적인 그룹 주체가 되며, 그룹 참여자들은 최소한의 정보로 그룹 참여허가를 원한다.

<11> 한편, 애드-혹망 무선 랜 시스템에 있어서는 그룹내에서 데이터의 기밀성 및 무결성 등의 통신보안을 위하여 데이터를 암호화하여 전송한다. 그런데, 애드-혹망의 특성상 암호화방식은 주로 대칭키를 이용한 암호화가 많이 이루어지며, 대칭키의 사용을 위해서는 도 1에 도시된 바와 같이 애드-혹망(10)을 구성하는 모든 무선단말들(11,13,15,17,19)이 공유키 값을 알고 있어야 하며, 그 값은 사용자들에 의해 설정되어진다. 따라서, 그룹내 모든 사용자들은 공유키 값을 사전에 숙지하고 있어야 하며, 이로 인해 사용상의 불편함을 야기시킨다. 또한, 사용자들이 공유키 값을 이미 알고 있더라도, 공유키 값이 수시로 변하지 않으면 공유키가 공격자들에게 드러날 가능성이 크다. 따라서, 공유키 값이 수시로 생성/분배/변경되어야 하는데, 현재의 애드-혹망에서는 이러한 기능을 담당할 주체가 없으므로 악의적인 주체에 의해 공격당할 가능성이 큰 문제점이 있다.

【발명이 이루고자 하는 기술적 과제】

<12> 따라서 본 발명의 목적은 상술한 문제점을 해결하기 위한 것으로서, 애드-혹망 무선 랜 시스템에 있어서 사용빈도가 적은 제1 공유키를 그룹 패스워드를 이용하여 생성하고, 데이터전송시 사용되는 제2 공유키를 랜덤 키 생성 알고리즘에 따라서 키분배센터 역할을 하는 무선단말에서 생성/분배/변경함으로써 데이터의 비밀성을 보장할 수 있는 이중키를 이용한 암호화방법을 제공하는데 있다.

<13> 본 발명의 다른 목적은 제1 공유키 및 제2 공유키로 이루어진 이중키를 이용하여 암호화함으로써 보안을 강화시킨 무선 랜 시스템을 제공하는데 있다.

【발명의 구성 및 작용】

- <14> 상기 목적을 달성하기 위하여 무선 랜 시스템에 있어서 본 발명에 따른 이중키를 이용한 암호화방법은 하나의 애드-혹 그룹을 구성하는 N개의 무선단말(여기서 N은 2 이상의 양수)중 키분배센타 역할을 담당하는 메인 무선단말을 설정하는 단계; 상기 N개의 무선단말에서 그룹 패스워드를 이용하여 제1 공유키를 생성하는 제1 공유키 생성단계; 상기 메인 무선단말에서 무선단말들간의 데이터 전송시 사용되는 제2 공유키를 생성하는 제2 공유키 생성단계; 상기 메인 무선단말에서 상기 제2 공유키를 상기 제1 공유키로 암호화하여 (N-1)개의 무선단말로 전송하는 제2 공유키 전송단계; 및 상기 N개의 무선단말간에 상기 제2 공유키로 데이터를 암호화하여 전송하는 데이터 전송단계를 포함하는 것을 특징으로 한다.
- <15> 상기 이중키를 이용한 암호화방법은 바람직하게로는 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체로 구현할 수 있다.
- <16> 상기 다른 목적을 달성하기 위하여 무선 랜 시스템에 있어서 본 발명에 따른 무선 랜 시스템은 하나의 애드-혹 그룹에서 키분배센타 역할을 담당하는 메인 무선단말과, (N-1)(여기서 N은 2 이상의 양수)개의 무선단말을 포함하며, 상기 N개의 무선단말 각각에 구비되며, 사용자로부터 입력되는 그룹 패스워드를 이용하여 제1 공유키를 생성하는 제1 공유키생성부; 상기 (N-1)개의 무선단말 각각에 구비되어, 상기 제1 공유키생성부로부터 제1 공유키를 저장하고, 제2 공유키 요청메시지를 상기 제1 공유키로 암호화하고, 상기 메인 무선단말로부터 제2 공유키 응답메시지를 상기 제1 공유키로 복호화하고, 사용자로부터 입력되는 데이터를 제2 공유키로 암호화하는 제1 암호화부; 상기 (N-1)개의 무선단말 각각에 구비되어, 상기 제2 공유키 요청메시지를 발생하여 상기

제1 암호화부로 출력하고, 상기 제1 암호화부에서 복호화된 제2 공유키 응답메시지로부터 제2 공유키를 추출하여 상기 제1 암호화부로 출력하는 제1 키관리부; 상기 메인 무선단말에 구비되어, 상기 제1 공유키생성부로부터 제1 공유키를 저장하고, 상기 제1 암호화부로부터 전송된 제2 공유키 요청메시지를 상기 제1 공유키로 복호화하고, 제2 공유키 응답메시지를 상기 제1 공유키로 암호화하여 상기 제1 암호화부로 전송하고, 사용자로부터 입력되는 데이터를 상기 제2 공유키로 암호화하는 제2 암호화부; 및 상기 메인 무선단말에 구비되어, 상기 제2 암호화부에서 복호화된 제2 공유키 요청메시지를 입력으로 하여 상기 제2 공유키를 생성하고, 생성된 제2 공유키를 포함하는 상기 제2 공유키 응답메시지를 상기 제2 암호화부로 출력하는 제2 키관리부를 포함하는 것을 특징으로 한다.

<17> 이하, 첨부된 도면을 참조하여 본 발명의 바람직한 실시예에 대하여 상세하게 설명하기로 한다.

<18> 도 2는 애드혹망 무선 랜 시스템에 있어서 본 발명에 따른 이중키를 이용한 암호화 방법을 설명하는 흐름도로서, 메인 무선단말 설정단계(21), 제1 공유키 생성단계(22), 제2 공유키 생성단계(23), 제2 공유키 전송단계(27) 및 데이터 전송단계(28)로 이루어진다.

<19> 도 2를 참조하면, 단계 21에서는 하나의 애드-혹 그룹을 구성하는 N개의 무선단말(여기서 N은 2 이상의 양수)중 키분배센터(Key Distribution Center, KDC) 역할을 담당하는 메인 무선단말을 설정하는데, 초기에는 애드-혹 그룹의 생성주체로 설정된다. 한편, 메인 무선단말이 애드-혹 그룹을 탈퇴하고자 하는 경우에는 그룹내 (N-1)개의 무선단말중 임의의 무선단말에게 키분배센터 역할을 이관시킬 수 있다.

- <20> 단계 22에서는 N개의 무선단말에서 그룹 패스워드를 이용하여 제1 공유키(LSK)를 생성한다. 단계 23에서는 메인 무선단말에서 무선단말들간의 데이터 전송시 사용되는 제2 공유키(SSK)를 생성하는데, 이를 좀 더 세부적으로 살펴보면, 단계 24에서는 단계 22에서 제1 공유키가 생성되면, 각 무선단말로부터 제2 공유키 요청메시지를 제1 공유키로 암호화하여 메인 무선단말로 전송하고, 단계 25에서는 메인 무선단말에서 제1 공유키를 이용하여 제2 공유키 요청메시지를 복호화하고, 단계 26에서는 복호화된 제2 공유키 요청메시지에 따라서 메인 무선단말에서 제2 공유키를 생성한다. 단계 22 및 단계 26에서는 일반화된 키 생성 알고리즘을 이용하여 제1 공유키 또는 제2 공유키를 생성할 수 있다.
- <21> 단계 27에서는 메인 무선단말에서 생성된 제2 공유키를 제1 공유키로 암호화하여 (N-1)개의 무선단말로 전송하고, 단계 28에서는 N개의 무선단말간에 제2 공유키로 데이터를 암호화하여 전송한다.
- <22> 한편, 도 3은 본 발명에 따른 제2 공유키 변경방법을 설명하는 플로우차트로서, 단계 31에서는 메인 무선단말에서 변경주기를 설정하면, 설정된 소정의 변경주기로 메인 무선단말에서 제2 공유키를 변경한다. 이와 같은 제2 공유키 변경도 도 2의 단계 26에서와 마찬가지로 일반화된 키 생성 알고리즘에 의해 가능하다. 단계 32에서는 메인 무선단말에서 변경된 제2 공유키를 변경전의 제2 공유키로 암호화하여 (N-1)개의 무선단말로 전송하고, 단계 33에서는 메인 무선단말로부터 변경된 제2 공유키를 변경전의 제2 공유키로 복호화하여 차후의 각 무선단말간의 데이터 전송에 암호화키로 사용한다.
- <23> 이와 같이 소정의 변경주기에 따라서 제2 공유키를 변경시키는 것에 의해, 메인 무선단말(45)에서 생성된 제2 공유키를 일정한 기간만 사용하고 소멸시키는 이유는 공격자

에 의한 암호분석을 방지하고, 공격자가 각 무선단말에 보관된 제2 공유키를 알아내는 것을 방지할 수 있다.

<24> 도 4는 본 발명에 따른 애드-혹망 무선 랜 시스템을 보여주는 세부블럭도로서, 크게 N개의 무선단말로 이루어지는 하나의 애드-혹 그룹에서 키분배센타 역할을 담당하는 메인 무선단말(45)과, (N-1)개의 서브 무선단말(41)을 포함한다. 여기서, N은 2 이상의 양수인 것이 바람직하다.

<25> 여기서, 서브 무선단말(41)은 제1 공유키 생성부(42), 제1 암호화부(43)와 제1 키관리부(44)를 포함하고, 메인 무선단말(45)은 제1 공유키 생성부(46), 제2 암호화부(47)와 제2 키관리부(44)를 포함한다. 초기에는 애드-혹 그룹의 생성주체로 메인 무선단말(45)이 설정되나, 메인 무선단말(45)이 애드-혹 그룹을 탈퇴하고자 하는 경우에는 그룹 내 (N-1)개의 무선단말 중 임의의 무선단말에게 키분배센타 역할을 이관시킬 수 있기 때문에 키분배센타 기능은 메인 무선단말(45) 뿐만 아니라 애드-혹 그룹을 구성하는 나머지 무선단말(41)이 모두 구비하도록 한다.

<26> 메인무선단말(45)은 서브 무선단말(41)과 마찬가지로 제1 공유키 생성부(46), 제2 암호화부(47)와 제2 키관리부(48)를 포함한다.

<27> 이와 같이 구성되는 애드-혹망 무선 랜 시스템의 동작을 도 5와 결부시켜 순차적으로 설명하기로 한다.

<28> 도 4 및 도 5에 있어서, 서브무선단말(41)의 제1 공유키 생성부(42)는 사용자로부터 입력되는 그룹 패스워드(411)를 이용하여 제1 공유키(LSK, 412)를 생성하여, 제1 암호화부(43)로 출력한다. 또한, 메인무선단말(45)의 제1 공유키 생성부(46)도 서브 무선단

말(41)에서와 마찬가지로 사용자로부터 입력되는 그룹 패스워드(451)를 이용하여 동일한 제1 공유키(LSK, 452)를 생성하여, 제2 암호화부(47)로 출력한다. 이때, 제1 공유키(LSK, 412, 452)는 일반적인 키 생성 알고리즘에 의해 생성할 수 있고, 이는 이 분야의 당업자에게는 자명한 사실이다.

<29> 제1 키관리부(44)에서는 제1 공유키생성부(42)에서 제1 공유키(LSK)가 생성되었음이 인식되면 제2 공유키(SSK) 요청메시지를 생성한다. 생성된 제2 공유키 요청메시지(413)는 제1 암호화부(43)로 공급된다.

<30> 제1 암호화부(43)는 제1 공유키생성부(42)로부터 공급되는 제1 공유키(412)를 저장하고 있으며, 제1 키관리부(44)에서 생성된 제2 공유키(SSK) 요청메시지(413)를 입력받아 저장되어 있는 제1 공유키(LSK)로 암호화하여 무선채널을 통해 메인무선단말(45)의 제2 암호화부(47)로 전송한다.

<31> 메인무선단말(45)에 있어서, 제2 암호화부(47)는 제1 공유키생성부(46)로부터 공급되는 제1 공유키(452)를 저장하고 있으며, 서브 무선단말(41)로부터 전송되는 암호화된 제2 공유키 요청메시지를 제1 공유키로 복호화한다. 복호화된 제2 공유키 요청메시지(453)는 제2 키관리부(48)로 공급된다.

<32> 제2 키관리부(48)는 제2 암호화부(47)에서 복호화된 제2 공유키 요청메시지(453)를 입력으로 하여 제2 공유키(SSK1)를 생성하고, 생성된 제2 공유키(SSK1)를 포함하는 제2 공유키 응답메시지(453)를 제2 암호화부(47)로 공급한다. 여기서, 제2 공유키(SSK1) 역시 일반적인 랜덤 키 생성 알고리즘을 이용하여 생성될 수 있다. 제2 암호화부(47)는 제2 공유키 응답메시지를 제1 공유키(LSK)로 암호화하여 무선채널을 통해 제1 암호화부(43)로 전송한다.

- <33> 다시 서브무선단말(41)로 돌아가서, 제1 암호화부(43)는 메인 무선단말로부터 전송된 암호화된 제2 공유키 응답메시지를 제1 공유키로 복호화하여 제1 키관리부(44)로 공급한다. 제1 키관리부(44)는 복호화된 제2 공유키 응답메시지(413)로부터 제2 공유키(SSK1)를 추출하고, 추출된 제2 공유키(SSK1,414)를 제1 암호화부(43)로 공급한다. 제1 암호화부(43)는 이후 사용자로부터 입력되는 데이타(415)를 제2 공유키(SSK1,414)로 암호화하여 전송하게 된다. 또한, 메인무선단말(45)에 있어서 제2 암호화부(47)도 이후 사용자로부터 입력되는 데이타(455)를 제2 공유키(SSK1,454)로 암호화하여 전송하게 된다.
- <34> 한편, 메인무선단말(45)의 제2 키관리부(48)에서는 일정한 변경주기를 설정하고, 변경주기에 따라 랜덤 키 생성 알고리즘을 이용하여 변경된 제2 공유키(SSK2)를 생성하여, 변경된 제2 공유키(SSK2)를 포함하는 제2 공유키 변경메시지(454)을 제2 암호화부(47)로 공급한다. 제2 암호화부(47)에서는 제2 공유키 변경메시지를 변경전의 제2 공유키(SSK1)로 암호화하여 무선채널을 통해 제1 암호화부(43)로 전송한다.
- <35> 제1 암호화부(43)에서는 암호화된 제2 공유키 변경메시지를 변경전의 제2 공유키(SSK1)로 복호화하여 제1 키관리부(44)로 공급하고, 제1 키관리부(44)에서는 복호화된 제2 공유키 변경메시지(413)로부터 변경된 제2 공유키(SSK2)를 추출하고, 추출된 제2 공유키(SSK2,414)를 제1 암호화부(43)로 공급한다. 제1 암호화부(43)는 이후 사용자로부터 입력되는 데이타(415)를 제2 공유키(SSK2,414)로 암호화하여 전송하게 된다. 또한, 메인무선단말(45)에 있어서 제2 암호화부(47)도 이후 사용자로부터 입력되는 데이타(455)를 제2 공유키(SSK2,454)로 암호화하여 전송하게 된다.

<36> 한편, 상술한 본 발명의 실시예들은 컴퓨터에서 실행될 수 있는 프로그램으로 작성 가능하고, 컴퓨터로 읽을 수 있는 기록매체를 이용하여 상기 프로그램을 동작시키는 범용 디지털 컴퓨터에서 구현될 수 있다. 상기 컴퓨터로 읽을 수 있는 기록매체는 예컨대 롬, 플로피 디스크, 하드디스크 등과 같은 마그네틱 저장매체, 예컨대 씨디롬, 디브이디 등과 같은 광학적 판독매체, 및 예컨대 인터넷을 통한 전송과 같은 캐리어 웨이브와 같은 저장매체를 포함한다.

【발명의 효과】

<37> 상술한 바와 같이 상술한 바와 같이 본 발명에 따르면, 애드-혹망 무선 랜 시스템에 있어서, 제1 공유키를 간편하고 사용하기 편리한 그룹 패스워드를 이용하여 생성함으로써 사용자의 편리성을 도모할 수 있고, 데이터전송시 사용되는 제2 공유키를 랜덤 키 생성 알고리즘에 따라서 키분배센터 역할을 하는 무선단말에서 생성/분배/변경함으로써 대칭키 알고리즘에서 키관리상의 번거로움을 해소시킬 수 있다.

<38> 또한, 제1 공유키는 사용빈도가 극히 적고, 제2 공유키는 일정한 변경주기로 변경시켜 줌으로써 악의적인 주체에 의해 공격당할 가능성을 감소시켜 그룹내 데이터의 비밀성이 보장될 수 있다.

<39> 또한, 초기에는 애드-혹 그룹의 생성주체인 무선단말이 키분배센터 역할을 담당하도록 하고, 해당 단말이 망 탈퇴시 다른 무선단말에게 키분배센터 역할을 이관시킴으로써 제2 공유키의 생성/분배/변경에 관련된 키관리를 지속적으로 할 수 있다.

<40> 본 발명에 대해 상기 실시예를 참고하여 설명하였으나, 이는 예시적인 것에 불과하며, 본 발명에 속하는 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및

균등한 타 실시예가 가능하다는 점을 이해할 것이다. 따라서 본 발명의 진정한 기술적 보호범위는 첨부된 특허청구범위의 기술적 사상에 의해 정해져야 할 것이다.

【특허청구범위】**【청구항 1】**

하나의 애드-혹 그룹을 구성하는 N개의 무선단말(여기서 N은 2 이상의 양수)중 키 분배센타 역할을 담당하는 메인 무선단말을 설정하는 단계;

상기 N개의 무선단말에서 그룹 패스워드를 이용하여 제1 공유키를 생성하는 제1 공유키 생성단계;

상기 메인 무선단말에서 무선단말들간의 데이터 전송시 사용되는 제2 공유키를 생성하는 제2 공유키 생성단계;

상기 메인 무선단말에서 상기 제2 공유키를 상기 제1 공유키로 암호화하여 (N-1)개의 무선단말로 전송하는 제2 공유키 전송단계; 및

상기 N개의 무선단말간에 상기 제2 공유키로 데이터를 암호화하여 전송하는 데이터 전송단계를 포함하는 것을 특징으로 하는 무선 랜 시스템에 있어서 이중키를 이용한 암호화방법.

【청구항 2】

제1 항에 있어서, 상기 메인 무선단말은 상기 애드-혹 그룹의 생성주체로 설정하는 것을 특징으로 하는 무선 랜 시스템에 있어서 이중키를 이용한 암호화방법.

【청구항 3】

제1 항에 있어서, 상기 메인 무선단말이 상기 애드-혹 그룹을 탈퇴할 경우에는 그룹내 (N-1)개의 서브 무선단말 중 임의의 서브 무선단말에게 키분배센타 역할을 이관시키는 것을 특징으로 하는 무선 랜 시스템에 있어서 이중키를 이용한 암호화방법.

【청구항 4】

제1 항에 있어서, 상기 방법은 설정된 소정의 변경주기로 상기 메인 무선단말에서 상기 제2 공유키를 변경하고, 변경된 제2 공유키를 변경전의 제2 공유키로 암호화하여 상기 (N-1)개의 서브 무선단말로 전송하는 제2 공유키 변경단계를 더 포함하는 것을 특징으로 하는 무선 랜 시스템에 있어서 이중키를 이용한 암호화방법.

【청구항 5】

제1 항에 있어서, 상기 제2 공유키 생성단계는

상기 제1 공유키가 생성되면, 상기 각 서브 무선단말로부터 제2 공유키 요청메시지를 상기 제1 공유키로 암호화하여 상기 메인 무선단말로 전송하는 단계;

상기 메인 무선단말에서 상기 제1 공유키를 이용하여 상기 제2 공유키 요청메시지를 복호화하는 단계; 및

상기 복호화된 제2 공유키 요청메시지에 따라서 상기 메인 무선단말에서 제2 공유키를 생성하는 단계로 이루어지는 것을 특징으로 하는 무선 랜 시스템에 있어서 이중키를 이용한 암호화방법.

【청구항 6】

제1 항 내지 제5 항 중 어느 한 항에 기재된 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

【청구항 7】

하나의 애드-혹 그룹에서 키분배센타 역할을 담당하는 메인 무선단말과, (N-1)(여기서 N은 2 이상의 양수)개의 서브 무선단말을 포함하며,



상기 N개의 무선단말 각각에 구비되며, 사용자로부터 입력되는 그룹 패스워드를 이용하여 제1 공유키를 생성하는 제1 공유키생성부;

상기 (N-1)개의 서브 무선단말 각각에 구비되어, 상기 제1 공유키생성부로부터 제1 공유키를 저장하고, 제2 공유키 요청메시지를 상기 제1 공유키로 암호화하고, 상기 메인 무선단말로부터 제2 공유키 응답메시지를 상기 제1 공유키로 복호화하고, 사용자로부터 입력되는 데이터를 제2 공유키로 암호화하는 제1 암호화부;

상기 (N-1)개의 서브 무선단말 각각에 구비되어, 상기 제2 공유키 요청메시지를 발생하여 상기 제1 암호화부로 출력하고, 상기 제1 암호화부에서 복호화된 제2 공유키 응답메시지로부터 제2 공유키를 추출하여 상기 제1 암호화부로 출력하는 제1 키관리부;

상기 메인 무선단말에 구비되어, 상기 제1 공유키생성부로부터 제1 공유키를 저장하고, 상기 제1 암호화부로부터 전송된 제2 공유키 요청메시지를 상기 제1 공유키로 복호화하고, 제2 공유키 응답메시지를 상기 제1 공유키로 암호화하여 상기 제1 암호화부로 전송하고, 사용자로부터 입력되는 데이터를 상기 제2 공유키로 암호화하는 제2 암호화부; 및

상기 메인 무선단말에 구비되어, 상기 제2 암호화부에서 복호화된 제2 공유키 요청메시지를 입력으로 하여 상기 제2 공유키를 생성하고, 생성된 제2 공유키를 포함하는 상기 제2 공유키 응답메시지를 상기 제2 암호화부로 출력하는 제2 키관리부를 포함하는 것을 특징으로 하는 무선 랜 시스템.

【청구항 8】

제7 항에 있어서, 상기 메인 무선단말은 상기 애드-혹 그룹의 생성주체로 설정하는 것을 특징으로 하는 무선 랜 시스템.

【청구항 9】

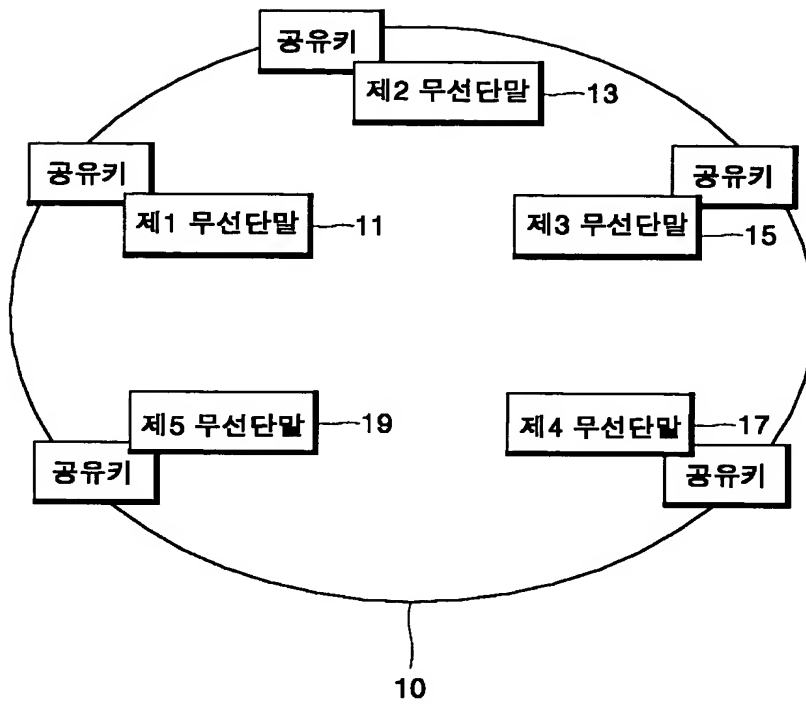
제7 항에 있어서, 상기 메인 무선단말이 상기 애드-혹 그룹을 탈퇴할 경우에는 그룹내 (N-1)개의 서브 무선단말 중 임의의 서브 무선단말에게 키분배센타 역할을 이관시키고, 이관받은 서브 무선단말이 상기 메인 무선단말로 동작하는 것을 특징으로 하는 무선 랜 시스템.

【청구항 10】

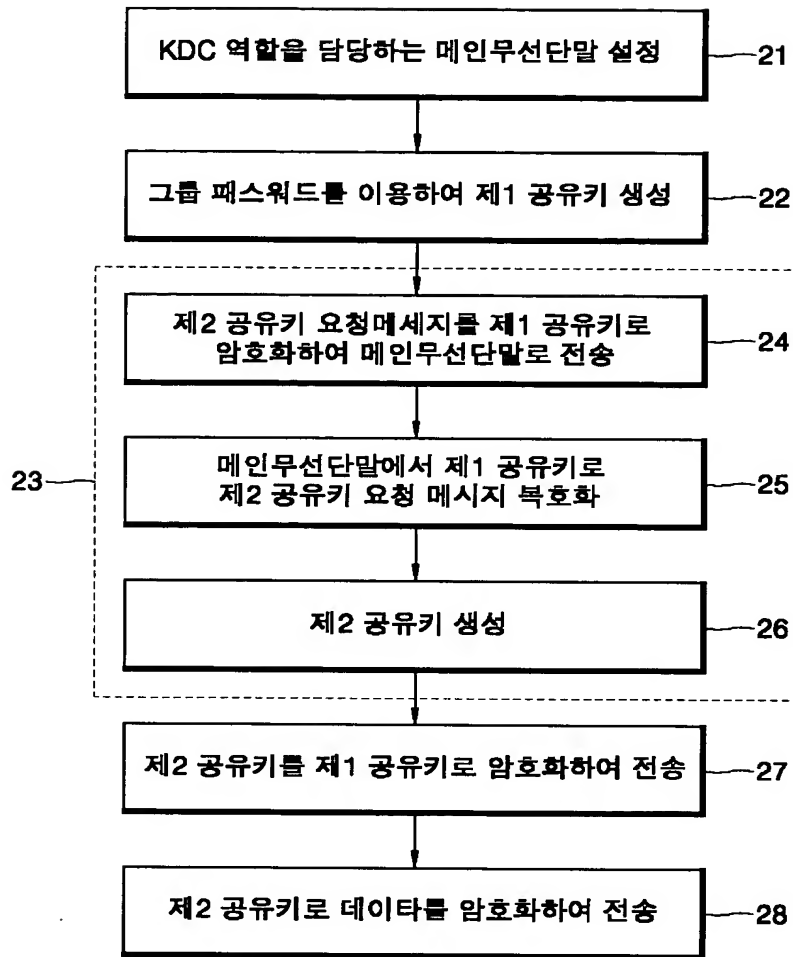
제7 항 내지 제9 항 중 어느 한 항에 있어서, 상기 메인 무선단말의 제2 키관리부에서는 설정된 변경주기로 상기 제2 공유키를 변경하고, 변경된 제2 공유키를 변경전의 제2 공유키로 암호화하여 상기 서브 무선단말의 제1 암호화부로 전송하는 것을 특징으로 하는 무선 랜 시스템.

【도면】

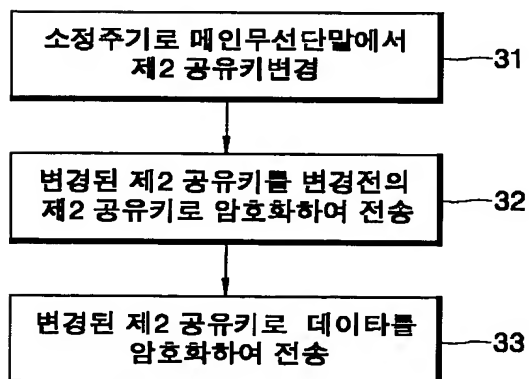
【도 1】



【도 2】



【도 3】



```

graph TD
    subgraph 41
        42[제1 공유키 생성부]
        44[제1 키 관리부]
        43[제1 암호화부]
        42 -- 412 --> 43
        44 <--> 43
        42 <--> 44
    end
    subgraph 45
        46[제1 공유키 생성부]
        48[제2 키 관리부 KDC]
        47[제2 암호화부]
        46 -- 452 --> 47
        48 <--> 47
        46 <--> 48
    end
    User1[사용자] -- 411 --> 42
    User1 -- 415 --> 46
    User2[사용자] -- 451 --> 46
    47 -- 455 --> 43

```

[illegible]